UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,806	03/15/2004	Jeffrey A. Von Arx	020.0328.US.UTL	1609

49475 7590 02/04/2009
CASCADIA INTELLECTUAL PROPERTY
500 UNION STREET
STE.1005
SEATTLE, WA 98101

EXAMINER	
KAPLAN, BENJAMIN A	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
02/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/800,806	VON ARX ET AL.	
	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-30 and 32-81* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-30 and 32-81* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the most recent papers filed on January 2, 2009.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 26, 2008 has been entered.

Response to Arguments and Amendments

3. The rejection of claims 1, 3-29, 60-68 and 79 under 35 USC § 101 is withdrawn.

4. Applicant's arguments filed January 2, 2009 have been fully considered but they are not persuasive.

Applicant arguments revolve primarily around the combination of Thompson and Griffiths and that the other references found in the rejections fail to make up the deficiencies in the combining of Thompson and Griffiths.

Applicant in substance that argues that "Thompson teaches providing corresponding keys to two devices, rather than maintaining a crypto key uniquely associated with an implantable medical device."

One of the device Thompson is providing a "corresponding key" to is a implantable medical device. The key that is held by that implantable medical device has been uniquely associated with it as it is that key that the implantable medical device is using to communicate with the second device without the public being able to determine what is being communicated.

Applicant in substance further argues that argues that Griffiths "fails to specifically show an implantable medical device for which for which a uniquely associated crypto key is maintained."

Examiner acknowledges that Griffiths dose not make any mention of an implantable medical device and is relying on Thompson to show that feature

Applicant in substance lastly argues that there is no motivation to combine Thompson and Griffiths.

While Griffiths does not its self necessarily have statements indicating its suitability for having an implantable medical device system added to it the combination is based on adding Griffiths' teaching to Thompson's method as apposed to the other way around. In this case the motivation has been provided by Thompson:

(Thompson, Column 8, Lines 54-59 "If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

Thompson on its own has specifically recognized the need for "additional security measures" to protect the "disbursement of the keys" where Griffiths provides a solution to Thompson's specific needs.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 30-39, 46-49, 56-58, are non-statutory because they are neither tied to a specific machine no result in a transformation of mater.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 1, 3-10, 17-20, 27-30, 32-39, 46-49, 56-61, 68-70, 77 & 78 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No.: 7,027,872 B2 (Thompson) in view of United States Patent No.: 7,136,999 B1 (Griffiths).

As Per Claim 1: Thompson teaches:

An apparatus for securely authenticating a data exchange session with an implantable medical device, comprising:

- a secure key repository comprising a memory and configured to maintain a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session

(Thompson, Column 8, Lines 18-50 "FIG. 4 is a block diagram illustrating one embodiment of a secure data transfer structural scheme in accordance with the present invention, shown generally at 220. In this embodiment, sensitive information 221 (such as patient information) is transferred in encrypted form from IMD any one of the programmers and instruments (112, 114, 116) or similar remote device to remote expert data center or clinician computer 122 across data communications media/connection 226. While a representative use of the present invention is illustrated using communications between Programmer (112, 114, 116) and clinician computer 122, any combination of clinician devices, IMD interface devices, central database or expert system servers, medical device personnel personal computers or servers, and patient monitoring equipment, or any other data transmission device may be used in accordance with the present invention. In the illustrative example, Programmer (112, 114, 116) may be any instrument capable of obtaining, storing, and transmitting medical and administrative information, including sensitive information 221. Programmer (112, 114, 116) is capable of being coupled to one or more IMDs 132. IMD 132 obtains certain information, possibly including sensitive information 221 from the patient, then

transfers the patient information to programmer (112, 114, 116). Data communication media 226 could be configured to include a telephone line connection, a direct network connection, an intranet connection, an internet connection, wireless LAN, fiber optic network a satellite connection, a laser or infrared system, any other suitable network protocol connection, or a combination thereof.

Key source 228 provides both programmer (112, 114, 116) and clinician computer 122 with encryption/decryption keys for encrypting/decrypting sensitive information 221.").

A device maintaining an encryption/decryption key has a repository for it.

- an external device configured to establish a secure connection through a first (a short range) interface with the secure key repository, to authenticate authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository

(Thompson, Column 8, Lines 48-59 "Key source 228 provides both programmer (112, 114, 116) and clinician computer 122 with encryption/decryption keys for encrypting/decrypting sensitive information 221. In one embodiment of the invention, key source 228 distributes symmetric encryption/decryption keys. In another embodiment of the invention, key source 228 distributes asymmetric keys (i.e., pubic/private keys). If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be

taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

- to transact the data exchange session using the crypto key to authenticate the data by transitioning to a second (a long range) interface

(Thompson, Column 9, Lines 10-16 "Before sensitive information 221 is transmitted across data communication media 226, sensitive information 221 is encrypted by encryption engine 230. Encryption engine 230 may be implemented in hardware or software, although may preferably be implemented in software to allow for ease of upgrades to different algorithms, key lengths, and key variation.").

(Thompson, Figure 4

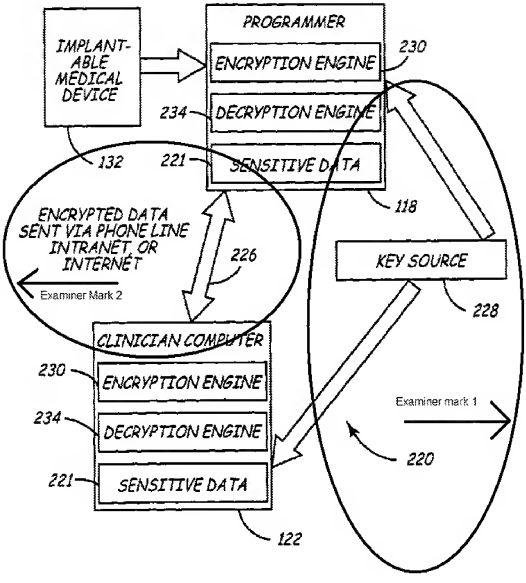

FIG. 4

).

Thompson does not explicitly teach that:

- the key exchange is done though a short range interface to transition to a long range interface

However Griffiths in analogous art does teach the above limitation:

(Griffiths, Claim 1 "A method of authenticating first and second electronic devices, comprising:

upon link set-up over a short-range wireless link, executing an authentication protocol by exchanging authentication information between the first and second electronic devices to initially authenticate communication between the first and second devices;

later, when the first and second electronic devices are beyond the short-range wireless link, executing the authentication protocol by exchanging the authentication information between the first and second electronic devices over an alternate communications link, then only allowing communication between the first and second devices if the first and second devices had initially been successfully authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Griffiths in to the method of Thompson because (Thompson, Column 8, Lines 54-59 "If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

As Per Claim 3: The rejection of claim 1 is incorporated and further Thompson teaches:

- an authentication component configured to employ the crypto key during the data exchange session, comprising at least one of:

- a command authenticator to authenticate commands exchanged through the external device with the implantable medical device and

(Thompson, Column 4, Lines 23-48 wherein medical device program commands" are encrypted and sent to the IMD).

- a data integrity checker configured to check the integrity of the data received by and transmitted from the external device

(Thompson, Column 4, Lines 49-66 message integrity checks).

- a data encrypter configured to encrypt the data received by and transmitted from the external device

(Thompson, Figure 4 both the Programmer and the Clinician computer have encryption engines and decryption engines).

As Per Claim 4: The rejection of claim 1 is incorporated and further Thompson does not explicitly teach the following limitations however Griffiths in analogous art does teach the following limitations:

- a short range interface logically defining a secured area around the implantable medical device in which to establish the secure connection

- a long range interface logically defining a non-secured area extending beyond the secured area in which to transact the data exchange session

(Griffiths, Claim 1 "A method of authenticating first and second electronic devices, comprising:

upon link set-up over a short-range wireless link, executing an authentication protocol by exchanging authentication information between the first and second electronic devices to initially authenticate communication between the first and second devices;

later, when the first and second electronic devices are beyond the short-range wireless link, executing the authentication protocol by exchanging the authentication information between the first and second electronic devices over an alternate communications link, then only allowing communication between the first and second devices if the first and second devices had initially been successfully authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Griffiths in to the method of Thompson because (Thompson, Column 8, Lines 54-59 "If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

As Per Claim 5: The rejection of claim 1 is incorporated and further Thompson teaches:

- a key generator configured to statically generate the crypto key, and to persistently store the crypto key in the secure key repository

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys).

As Per Claim 6: The rejection of claim 5 is incorporated and further Thompson teaches:

- the crypto key is stored on at least one of the implantable medical device, a patient designator, a secure database, a physical token, and a repeater

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

As Per Claim 7: The rejection of claim 5 is incorporated and further Thompson teaches:

- the crypto key is securely retrieved from the secure key repository through a programmer

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

As Per Claim 8: The rejection of claim 1 is incorporated and further Thompson teaches:

- a key generator configured to dynamically generate the crypto key

(Thompson, Figure 4 key source 228, and column 8 lines 48-66 and column 910-49; the key source distributes many different kind of algorithms including the generation of session keys).

As Per Claim 9: The rejection of claim 8 is incorporated and further Thompson teaches:

- the crypto key is stored on at least one of the implantable medical device, a patient designator, and a repeater

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

As Per Claim 10: The rejection of claim 8 is incorporated and further Thompson teaches:

- the crypto key is securely retrieved from the secure key repository through at least one of a programmer and a repeater

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

As Per Claim 17: The rejection of claim 1 is incorporated and further Thompson teaches:

- a secure database configured to maintain the crypto key

(Thompson column 8 lines 18-47 teaches a secure database).

- a secure server configured to provide the crypto key through a secure connection

(Thompson column 9 lines 10-49 teaches a tunneled connection).

As Per Claim 18: The rejection of claim 17 is incorporated and further Thompson teaches:

- the secure connection comprises at least one of a serial or hardwired connection and a secure network connection

(Thompson column 9 lines 63-67 and column 10 lines 1-10 teach hardwired secure connection).

As Per Claim 19: The rejection of claim 17 is incorporated and further Thompson teaches:

- the external device comprises a programmer

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

As Per Claim 20: The rejection of claim 19 is incorporated and further Thompson teaches:

- the crypto key is provided from the programmer to a repeater

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

As Per Claim 27: The rejection of claim 1 is incorporated and further Thompson teaches:

- the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key

(Thompson column 9 lines 50-64 teaches "a 128 bit hashed representation of a message" and a public key).

As Per Claim 28: The rejection of claim 1 is incorporated and further Thompson teaches:

- the crypto key comprises at least one of a statically generated and persistently stored crypto key, dynamically generated and persistently stored crypto key, a dynamically generated and non-persistently stored session crypto key

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

As Per Claim 29: The rejection of claim 1 is incorporated and further Thompson teaches:

- the implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device

(Thompson column 2 lines 39-64 teach implantable cardiac devices).

As Per Claim 30: Claim 30 is substantially a restatement of the apparatus of claim 1 as a method and is rejected under substantially the same reasoning.

As Per Claim 32: The rejection of claim 30 is incorporated and further Claim 32 is substantially a restatement of the apparatus of claim 3 as a method and is rejected under substantially the same reasoning.

As Per Claim 33: The rejection of claim 30 is incorporated and further Claim 33 is substantially a restatement of the apparatus of claim 4 as a method and is rejected under substantially the same reasoning.

As Per Claim 34: The rejection of claim 30 is incorporated and further Claim 34 is substantially a restatement of the apparatus of claim 5 as a method and is rejected under substantially the same reasoning.

As Per Claim 35: The rejection of claim 34 is incorporated and further Claim 35 is substantially a restatement of the apparatus of claim 6 as a method and is rejected under substantially the same reasoning.

As Per Claim 36: The rejection of claim 35 is incorporated and further Claim 36 is substantially a restatement of the apparatus of claim 7 as a method and is rejected under substantially the same reasoning.

As Per Claim 37: The rejection of claim 30 is incorporated and further Claim 37 is substantially a restatement of the apparatus of claim 8 as a method and is rejected under substantially the same reasoning.

As Per Claim 38: The rejection of claim 37 is incorporated and further Claim 38 is substantially a restatement of the apparatus of claim 9 as a method and is rejected under substantially the same reasoning.

As Per Claim 39: The rejection of claim 37 is incorporated and further Claim 39 is substantially a restatement of the apparatus of claim 10 as a method and is rejected under substantially the same reasoning.

As Per Claim 46: The rejection of claim 30 is incorporated and further Claim 46 is substantially a restatement of the apparatus of claim 17 as a method and is rejected under substantially the same reasoning.

As Per Claim 47: The rejection of claim 46 is incorporated and further Claim 47 is substantially a restatement of the apparatus of claim 18 as a method and is rejected under substantially the same reasoning.

As Per Claim 48: The rejection of claim 46 is incorporated and further Claim 48 is substantially a restatement of the apparatus of claim 19 as a method and is rejected under substantially the same reasoning.

As Per Claim 49: The rejection of claim 48 is incorporated and further Claim 49 is substantially a restatement of the apparatus of claim 20 as a method and is rejected under substantially the same reasoning.

As Per Claim 56: The rejection of claim 30 is incorporated and further Claim 56 is substantially a restatement of the apparatus of claim 27 as a method and is rejected under substantially the same reasoning.

As Per Claim 57: The rejection of claim 30 is incorporated and further Claim 57 is substantially a restatement of the apparatus of claim 28 as a method and is rejected under substantially the same reasoning.

As Per Claim 58: The rejection of claim 30 is incorporated and further Claim 58 is substantially a restatement of the apparatus of claim 29 as a method and is rejected under substantially the same reasoning.

As Per Claim 59: Claim 59 is substantially a restatement of claim 1 and is rejected under substantially the same reasoning. An apparatus performing the indicated function inherently has a means for doing so.

As Per Claim 60: Thompson teaches:

An apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

- a first (a short range) interface device configured to provide communication with an implantable medical device by authenticating access to a securely maintained crypto key using a first (a short range) interface;

(Thompson, Column 8, Lines 48-59 "Key source 228 provides both programmer (112, 114, 116) and clinician computer 122 with encryption/decryption keys for encrypting/decrypting sensitive information 221. In one embodiment of the invention, key source 228 distributes symmetric encryption/decryption keys. In another embodiment of the invention, key source 228 distributes asymmetric keys (i.e., pubic/private keys). If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

- an external device configured to commence a data exchange session with the implantable medical device via a second (a long range) interface upon successful access authentication, and to transact the data exchange session using the crypto key

(Thompson, Column 9, Lines 10-16 "Before sensitive information 221 is transmitted across data communication media 226, sensitive information 221 is encrypted by encryption engine 230. Encryption engine 230 may be implemented in hardware or software, although may preferably be implemented in software to allow for ease of upgrades to different algorithms, key lengths, and key variation.").

(Thompson, Figure 4

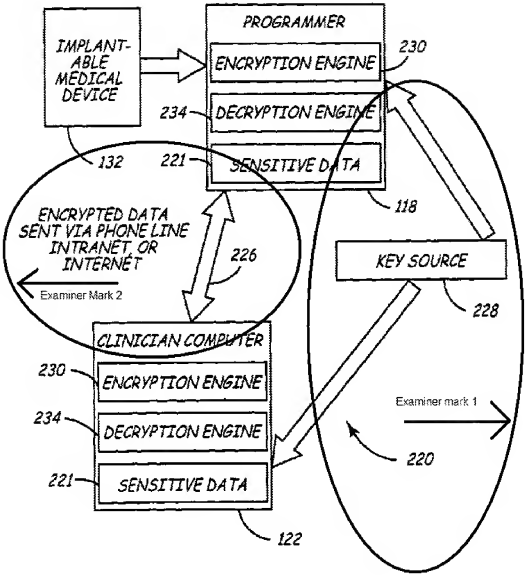

FIG. 4

).

Thompson does not explicitly teach that:

- the key exchange is done though a short range interface to transition to a long range interface

However Griffiths in analogous art does teach the above limitation:

(Griffiths, Claim 1 "A method of authenticating first and second electronic devices, comprising:

upon link set-up over a short-range wireless link, executing an authentication protocol by exchanging authentication information between the first and second electronic devices to initially authenticate communication between the first and second devices;

later, when the first and second electronic devices are beyond the short-range wireless link, executing the authentication protocol by exchanging the authentication information between the first and second electronic devices over an alternate communications link, then only allowing communication between the first and second devices if the first and second devices had initially been successfully authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Griffiths in to the method of Thompson because (Thompson, Column 8, Lines 54-59 "If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

As Per Claim 61: The rejection of claim 60 is incorporated and further Thompson teaches:

- the implantable medical device maintains patient health information in an encrypted form

(Thompson, column 10 lines 28-43, data is encrypted before exchanged).

As Per Claim 68: The rejection of claim 60 is incorporated and further Thompson teaches:

- the long range interface is augmented using one or more repeaters

(Thompson figure 1 programmer (extender) 112 and associated text).

As Per Claim 69: Claim 69 is substantially a restatement of the apparatus of claim 60 as a method and is rejected under substantially the same reasoning.

As Per Claim 70: The rejection of claim 69 is incorporated and further Claim 70 is substantially a restatement of the apparatus of claim 61 as a method and is rejected under substantially the same reasoning.

As Per Claim 77: The rejection of claim 69 is incorporated and further Claim 77 is substantially a restatement of the apparatus of claim 68 as a method and is rejected under substantially the same reasoning.

As Per Claim 78: Claim 78 is substantially a restatement of claim 60 and is rejected under substantially the same reasoning. An apparatus performing the indicated function inherently has a means for doing so.

8. Claim 79-81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson in view of Griffiths in further view of United States Patent No.: 6,442,432 B2 (Lee).

As Per Claim 79: Thompson teaches:

An apparatus for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

- a secure external device configured to request the crypto key from a secure server device via a first (a secure short range) connection based on the identification of and authentication to access the implantable medical device

(Thompson, Column 8, Lines 48-59 "Key source 228 provides both programmer (112, 114, 116) and clinician computer 122 with encryption/decryption keys for

encrypting/decrypting sensitive information 221. In one embodiment of the invention, key source 228 distributes symmetric encryption/decryption keys. In another embodiment of the invention, key source 228 distributes asymmetric keys (i.e., pubic/private keys). If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

- to receive the crypto key, to commence a data exchange session with the implantable medical device by transitioning to a second (a long range) interface upon successful access authentication, and to transact the data exchange session using the crypto key

(Thompson, Column 9, Lines 10-16 "Before sensitive information 221 is transmitted across data communication media 226, sensitive information 221 is encrypted by encryption engine 230. Encryption engine 230 may be implemented in hardware or software, although may preferably be implemented in software to allow for ease of upgrades to different algorithms, key lengths, and key variation.").

(Thompson, Figure 4

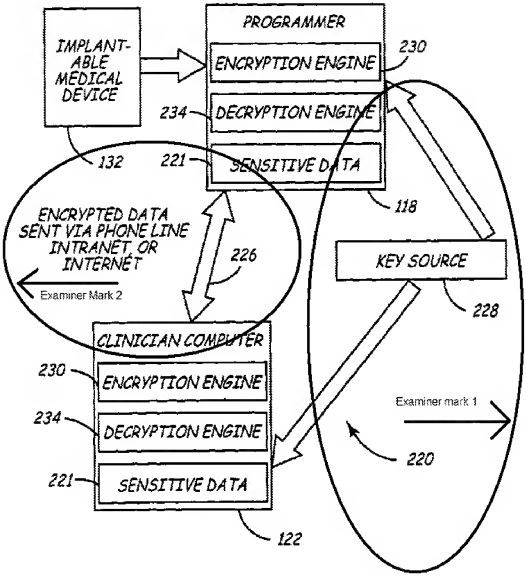

FIG. 4

).

- a securely maintained crypto key

(Thompson, Column 8, Lines 18-50 "FIG. 4 is a block diagram illustrating one embodiment of a secure data transfer structural scheme in accordance with the present invention, shown generally at 220. In this embodiment, sensitive information 221 (such as patient information) is transferred in encrypted form from IMD any one of the programmers and instruments (112, 114, 116) or similar remote device to remote expert data center or clinician computer 122 across data communications media/connection 226. While a representative use of the present invention is illustrated using communications between Programmer (112, 114, 116) and clinician computer 122, any combination of clinician devices, IMD interface devices, central database or expert system servers, medical device personnel personal computers or servers, and patient monitoring equipment, or any other data transmission device may be used in accordance with the present invention. In the illustrative example, Programmer (112, 114, 116) may be any instrument capable of obtaining, storing, and transmitting medical and administrative information, including sensitive information 221. Programmer (112, 114, 116) is capable of being coupled to one or more IMDs 132. IMD 132 obtains certain information, possibly including sensitive information 221 from the patient, then transfers the patient information to programmer (112, 114, 116). Data communication media 226 could be configured to include a telephone line connection, a direct network connection, an intranet connection, an internet connection, wireless LAN, fiber optic network a satellite connection, a laser or infrared system, any other suitable network protocol connection, or a combination thereof.

Key source 228 provides both programmer (112, 114, 116) and clinician computer 122 with encryption/decryption keys for encrypting/decrypting sensitive information 221.").

A device maintaining an encryption/decryption key has a repository for it.

Thompson does not explicitly teach that:

- the key exchange is done though a short range interface to transition to a long range interface

However Griffiths in analogous art does teach the above limitation:

(Griffiths, Claim 1 "A method of authenticating first and second electronic devices, comprising:

upon link set-up over a short-range wireless link, executing an authentication protocol by exchanging authentication information between the first and second electronic devices to initially authenticate communication between the first and second devices;

later, when the first and second electronic devices are beyond the short-range wireless link, executing the authentication protocol by exchanging the authentication information between the first and second electronic devices over an alternate communications link, then only allowing communication between the first and second devices if the first and second devices had initially been successfully authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Griffiths in to the method of

Thompson because (Thompson, Column 8, Lines 54-59 "If the encryption/decryption algorithms employed by the invention are standard algorithms known to the public, additional security measures must be taken in the disbursement of the keys from key source 228 to programmer (112, 114, 116) and 122 in order to ensure privacy.").

Thompson and Griffiths do not explicitly teach the following limitation:

- a secure server device configured to provide identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key

However Lee in analogous art does teach the above limitation:

(Lee, Column 16 lines 3-33 Authentication is preferably implemented end to end.).

It would be obvious to a person of ordinary skill in the art at the time of invention was made to incorporate use Lee's teachings of end to end authenticated communication with Thompson's method. In order to help insure that no access or information is unnecessarily provided to an unauthorized user.

As Per Claim 80: Claim 80 is substantially a restatement of the system of claim 79 as a method and is rejected under substantially the same reasoning.

As Per Claim 81: Claim 81 is substantially a restatement of the system of claim 79 as an apparatus and is rejected under substantially the same reasoning. An apparatus performing the indicated function inherently has a means for doing so.

9. Claim 11-16, 40-45, 62, 63, 65-67, 71, 72 & 74-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson in view of Griffiths in further view of United States Patent No.: 6,493,587 B1 (Eckmiller).

As Per Claims 11 and 12: The rejection of claim 1 is incorporated and further Thompson and Griffiths do not explicitly teach the following limitations however Eckmiller in analogous art does teach the following limitations:

- the crypto key is maintained on the implantable medical device, further comprising: a short range telemetry interface retrieving the crypto key through short range telemetry

- the short range telemetry comprises inductive telemetry

(Eckmiller column 9 lines 28-53, passes public key).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to utilize Eckmillers method of storing and retrieving keys because it offers the advantage of preventing the unauthorized access to important functions of neuroprostheses and unauthorized imitation of components (Eckmiller column 3 lines 5-15).

As Per Claim 13: The rejection of claim 11 is incorporated and further Thompson teaches:

- the external device comprises a programmer

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

As Per Claim 14: The rejection of claim 13 is incorporated and further Thompson teaches:

- the crypto key is provided from the programmer to a repeater

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer; and Thompson figure 1 programmer (extender) 112 is interpreted to be the repeater.

As Per Claim 15: The rejection of claim 11 is incorporated and further Thompson teaches:

- the external device comprises a patient designator

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer wherein the clinician computer is interpreted to be the patient designator).

As Per Claim 16: The rejection of claim 15 is incorporated and further Thompson teaches:

- the crypto key is provided from the patient designator to at least one of a programmer and a repeater

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer; within the asymmetric key algorithm the public key would be passed from the clinician computer to the programmer).

As Per Claims 40-45: The rejection of claim 30 is incorporated and further Claims 40-45 are substantially a restatement of the apparatuses of claims 11-16 as a method and are rejected under substantially the same reasoning.

As per Claim 62: The rejection of claim 60 is incorporated and further Thompson and Griffiths do not explicitly teach the following limitation however Eckmiller in analogous art does teach the following limitation:

- the access authentication occurs through short range telemetry, further comprising: a short range telemetric connection with the implantable medical device; a short range telemetric device configured to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device

(Eckmiller column 9 lines 28-53, passes public key).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to utilize Eckmillers method of storing and retrieving keys because it offers the advantage of preventing the unauthorized access to important functions of neuroprostheses and unauthorized imitation of components (Eckmiller column 3 lines 5-15).

As per Claim 63: The rejection of claim 60 is incorporated and further Thompson teaches:

- the patient designator configured to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer wherein the clinician computer is interpreted to be the patient designator).

Thompson and Griffiths do not explicitly teach the following limitation however Eckmiller in analogous art does teach the following limitation:

- a short range telemetric connection with the implantable medical device

(Eckmiller column 9 lines 28-53, passes public key).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to utilize Eckmillers method of storing and retrieving keys because it offers the advantage of preventing the unauthorized access to important functions of neuroprostheses and unauthorized imitation of components (Eckmiller column 3 lines 5-15).

As per Claim 65: The rejection of claim 60 is incorporated and further Thompson and Griffiths do not explicitly teach the following limitation however Eckmiller in analogous art does teach the following limitation:

- the implantable medical device maintains patient health information in an unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection

(Eckmiller column 9 lines 28-53, passes public key).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to utilize Eckmillers method of storing and retrieving keys because it offers the advantage of preventing the unauthorized access to important functions of

neuroprostheses and unauthorized imitation of components (Eckmiller column 3 lines 5-15).

As per Claim 66: The rejection of claim 65 is incorporated and further Thompson teaches:

- an external source configured to send a session crypto key to the implantable medical device

(Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer wherein the clinician computer is interpreted to be the patient designator); and

- an encrypter configured to encrypt the patient health information maintained in the implantable medical device

(Thompson, Figure 4 both the Programmer and the Clinician computer have encryption engines and decryption engines).

Thompson and Griffiths do not explicitly teach the following limitation however Eckmiller in analogous art does teach the following limitation:

- a short range telemetric connection with the implantable medical device

(Eckmiller column 9 lines 28-53, passes public key).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to utilize Eckmillers method of storing and retrieving keys because it offers the advantage of preventing the unauthorized access to important functions of neuroprostheses and unauthorized imitation of components (Eckmiller column 3 lines 5-15).

As per Claim 67: The rejection of claim 60 is incorporated and further Thompson teaches:

- an encrypter configured to encrypt patient health information maintained in the implantable medical device

(Thompson, Figure 4 both the Programmer and the Clinician computer have encryption engines and decryption engines).

Thompson and Griffiths do not explicitly teach the following limitation however Eckmiller in analogous art does teach the following limitation:

- the patient designator configured to establish a short range telemetric connection with the implantable medical device, and to send a session crypto key to the implantable medical device

(Eckmiller column 9 lines 28-53, passes public key)

As Per Claim 71: The rejection of claim 69 is incorporated and further Claim 71 is substantially a restatement of the apparatus of claim 62 as a method and is rejected under substantially the same reasoning.

As Per Claim 72: The rejection of claim 69 is incorporated and further Claim 72 is substantially a restatement of the apparatus of claim 63 as a method and is rejected under substantially the same reasoning.

As Per Claim 74: The rejection of claim 69 is incorporated and further Claim 74 is substantially a restatement of the apparatus of claim 65 as a method and is rejected under substantially the same reasoning.

As Per Claim 75: The rejection of claim 74 is incorporated and further Claim 75 is substantially a restatement of the apparatus of claim 66 as a method and is rejected under substantially the same reasoning.

As Per Claim 76: The rejection of claim 69 is incorporated and further Claim 76 is substantially a restatement of the apparatus of claim 67 as a method and is rejected under substantially the same reasoning.

10. Claim 21-26, 50-55, 64 & 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson in view of Griffiths in further view of United States Patent Application Publication No.: 2002/0016913 A1 (Wheeler et al.).

As Per Claim 21: The rejection of claim 1 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- a physical token configured to maintain the crypto key; and a reader configured to retrieve the crypto key by accessing the physical token

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claim 22: The rejection of claim 21 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- a physical label configured to specify the crypto key on the physical token

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claim 23: The rejection of claim 22 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- the physical label comprises at least one of alphanumeric text, bar coding, and an outwardly-appearing indication

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claim 24: The rejection of claim 21 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- internal storage configured to specify the crypto key on the physical token

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claim 25: The rejection of claim 24 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- the internal storage comprises at least one of a transistor, a memory circuit, an electronically readable storage medium, and a magnetically readable storage medium

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claim 26: The rejection of claim 21 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- the physical token is accessed using magnetic, optical, serial, and physical reading

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claims 50-55: The rejection of claim 30 is incorporated and further Claims 50-55 are substantially a restatement of the apparatuses of claims 21-26 as a method and are rejected under substantially the same reasoning.

As Per Claim 64: The rejection of claim 60 is incorporated and further Thompson does not explicitly teach the following limitations however Wheeler et al in analogous art does teach the following limitations:

- the access authentication occurs by using a physical token, further comprising: a physical token; and a reader to receive the crypto key from the physical token

(Wheeler et al., Paragraphs [0066] and [0279]).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate Wheeler et al.'s use of a smart card in to

Thompson's method. In order to enhance the level of security provided in Thompson's method.

As Per Claim 73: The rejection of claim 69 is incorporated and further Claim 73 is substantially a restatement of the apparatus of claim 64 as a method and is rejected under substantially the same reasoning.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434